ePrio

11/12/2007

To the Secretary of the Federal Trade Commission,
Room H-135 (Annex N)
600 Pennsylvania Av, N.W.
Washington, D.C., 20580

Subject: Ehavioral Advertising: Tracking, Targeting, Technology

Philippe Coueignoux holds a PhD in Electrical Engineering and Computer Science from MIT. He has more than ten years of experience in the field of "personalized Internet interactions in privacy" and has applied for several patents in this domain. The first one has been granted as US Patent no 6,092,197 and the last one has been recently submitted as US provisional application 60/973,565. Founder of ePrio Inc. and operator of the site eprivacy.com, Philippe Coueignoux is currently in the process of securing financing.

Philippe Coueignoux is also the author of "Philippe's Fillips", a weekly blog in defense of individuals' data rights, and "Vulnerabilities and Liabilities in the Information Age", an MBA level academic course, both published on eprivacy.com. The views defended by the author are independent from external influence. For the sake of disclosure, the author acknowledges however that his views are informed by the technologies he has developped, and naturally compatible with and favorable to, the commercial goals pursued by ePrio.

In these capacities, I wish to submit the following comments to your attention.

Beyond a doubt targeted advertising is a promising area for economic growth, as inferred from the valuations of some companies with plans in this field. Yet implementation plans call for collecting and aggregating personal profiles at a level of detail which threatens the privacy of individual consumers. To meet this threat while encouraging trade, a do-not-track registry is not efficient as proposed and therefore not advisable. However it is in the remit of the FTC to prevent companies involved in and benefiting from, targeted advertising from engaging in deceptive, abusive or discriminatory practices or abetting the rise of such practices.

To do so imposes neither a change in the present laws governing privacy nor the use of any particular technology. It is enough to require that

- against **deception**: consumers be able to verify what information is available on them for targeting purposes
- against **abuse of power**: a redress process exist to let consumers contest information held about them
- against **discrimination**: information which may lead to unlawful discrimination or intimidation be reliably isolated

Together these measures ensure that, under the current consumer protection laws and regulations whose application is entrusted to the FTC:

- those engaged in consumer online tracking and targeting are made responsible for their acts and their consequences
- any violation can be easily spotted either by the consumers themselves or by independent auditors

ePrio Inc. - 14 Barbara D Lane - Tewksbury, MA 01876 - Phone/Fax: 1-978-658-7801 - philippe.coueignoux@eprivacy.com

ePrio

In brief it is suggested that the FTC takes four measures, i.e.:

-1- requires any organization presenting a targeted ad to a consumer (a "presenter") to give this consumer free, concomitant, online access to the profile used for targeting, being understood that:

- this organization is the one with whom the consumer is currently aware of interacting online, not some subcontractor
- this profile is not restricted to the information actually used but rather includes all the information made available
- each elementary information included in this profile is to be:
    - reported in plain language in the language normally used by the consumer
    - with the date of its original collection, the name of and a contact at, the collecting entity ("the originator")
    - no more than 18 months old counting from the date of collection

-2- requires any presenter to set up a protest process which:

- clearly identify whether an elementary profile information may or may not, according to its originator, be modified by the consumer
- enable modifiable information to be updated or erased by the consumer during online profile perusal
- allow the consumer to challenge any other information through an FTC approved third party arbitrator paid by the originator, although, past a certain number per period, unsuccessful challenges may be charged to the consumer
- guarantee consumer-inspired updates persist for a minimum of 6 months, 18 months in case of arbitration

-3- requires any originator of any elementary information in a profile used for targeting ads to:

- keep a log of all copies made of this elementary information
- guarantee, upon receipt of a notification update from a consumer or an arbitrator, all copies of the previous information not controlled by the consumer be changed accordingly within 24 h

-4- forbids any presenter from using a profile for targeting if this profile contains any information which could be potentially used by the presenter or any third party to discriminate against a consumer on the basis of race, ethnic origin, gender, age, disabilities, sexual preferences, political or religious convictions or to intimidate a consumer with threats of revealing a shameful behavior such as an interest in adult entertainment, alcohol, drugs and gambling or a highly private matter such as a medical condition or a credit worthiness factor, unless:

- such a profile is inaccessible to any human being besides said consumer or the employees of an FTC approved third party ("an escrow"):
    - whose sole activity is to warehouse such profiles on the behalf of its clients
    - who operates at arm's length from advertisers, originators, presenters, their agents and intermediaries
- all targeting requests from advertisers bearing on such profiles can be automatically guaranteed to be in compliance with all applicable anti-discrimination laws
- the process insuring such automatic guarantees can be periodically and randomly audited by an FTC approved auditor at the expense of the presenters using the profiles thus protected.

The solution proposed is further detailed and explained in a separate attachment.

Respectfully yours,

Philippe Coueignoux PhD
President
ePrio Inc.

ePrio

suggestions to the Federal Trade Commission on ehavioral tracking and targeting

- a do-not-track registry is an ineffective solution to counter the threats to privacy

The existing do-not-call registry has been a resounding success. But setting up and using a registry is only part of the implementation. A do-not-do list is meant to prevent undesirable acts. To be effective a solution must also include the means to spot violations, gather the necessary evidence and prosecute the offenders successfully.

Contrary to the do-not-call registry, which prevents an end immediately apparent to the consumer it wrongs, a do-not-track registry would bear on means kept hidden from consumers.

Assume nevertheless a consumer rightly believes he or she has been tracked in violation of the registry. A do-not-call violation is easy to document since the offender is bent to identify itself to its victim as the violation occurs. In the case of a do-not-track violation, no one can say for sure a specific advertisement had been targeted as a result of a tracking violation. Random coincidences happen. Consumers will have to document whole suspicious strings of advertisements and, to prosecute an offender with any chance of success, the FTC will have to engage in extensive discoveries.

In practice consumers will not take the time and the FTC will not have the resources necessary to spot violations and gather evidence, making a do-not-track registry ineffective.

- what conditions should any solution satisfy?

I propose below a list of four conditions.

-1- fall within the FTC's remit.
-2- be independent of technology. Solutions specifying a technology fall in obsolescence and stiffle innovation
-3- respect economic principles. Costs must be born by those who benefit and commensurate with the benefits
-4- be practical. This can be divided into three imperatives:
  -a- establish effective responsibility, which makes violations easy to spot, document, report and prosecute
  -b- separate enforcement from profits. Wolves are simply not credible to look after the interests of sheep
  -c- be technically possible. Notice this condition is compatible with technology independence.

In view of these conditions, let us proceed to examine the solution previously outlined .

- measure 1: enabling the consumer - visibility

The best way to keep the costs down and the response effective is to make consumers the cornerstone of their own protection. This requires the underlying process to be visible to the consumer.

The threats to consumer privacy do not come from the act of advertising nor, in principle, from the act of selecting more appropriate ads. The most immediate threat is to be found in the means to achieve these ends, i.e. in the building of an evermore detailed personal profile. Anonymity is irrelevant since identification can be inferred from enough details as demonstrated by the public release last year of private search requests tracked by AOL. Therefore the profile gathered on a particular consumer for the purpose of targeted advertising must be made available to this consumer, which is measure 1.

ePrio Inc. - 14 Barbara D Lane - Tewksbury, MA 01876 - Phone/Fax: 1-978-658-7801 - philippe.coueignoux@eprivacy.com

When a targeted ad is presented to him or her, the consumer is only aware of the organization whose site he or she currently browses. This very organization, the presenter, is the one to benefit from presenting the ad and, according to our principles, must be the one responsible for letting the consumer access his or her profile.

Measure 1 further requires that profile access must be online, concomitant, free, readable by the consumer and flag each elementary information with its date of collection, name of the originator and means of contact. This is necessary to ensure measure 1 is practical, avoiding obfuscation by sources and allowing verification by consumers. The implementation cost is minimal since this information should already exist. In particular no presenter should be allowed to profit on anonymous tips and tracking should reveal the consumer preferred language as a matter of course.

The final requirement that no information be more than 18 months old is in line with pledges already made by Google to the European Commission to protect consumer privacy.

Notice that violations of measure 1 are easy to track down. Independent watchdogs can publish a list of presenters. Individual consumers can easily check that a known presenter does indeed provides access to their specific profiles and that these profiles contain the required information. Denying a consumer access to his or her profile would be a violation similar to calling a registered do-not-call consumer. Faking entries in such a consumer profile, e.g. pretending it is empty when it is not, would constitute fraud and face criminal prosecution.

- measures 2 and 3: enabling the consumer - redress

Tracking and targeting are part of a body of engineering called pattern recognition. A fundamental lesson of this field teaches that errors do occur. Besides technical glitches and human errors, all networked endeavors are prey to third party attacks. While errors are not violations in themselves, it is incumbent to presenters and orginators to make sure such errors can be promptly eliminated by allowing consumers to edit their profile online, either providing the correct data or erasing the data altogether.

Since consumers are liable to be less than truthful themselves, the originator of an information should be allowed to stand by one's facts and mark any elementary information it so chooses as privileged, e.g. an information relative to credit worthiness. Consumers may still read but not edit such privileged information.

Since conflicts on privileged information are unavoidable, they are resolved by independent arbitrators, approved by the FTC and paid by the originators, who are the ones who benefit from the information they collect. Originators are free to avoid both complexity and cost by claiming no privilege on information. Presumably some will seek to privilege information for the sake of extracting higher prices from aggregators and advertisers.

Overly litigious consumers should be made to bear the costs of their frivolity and pay for lost arbitration costs if they lose too many arbitrations within a certain time span.

The presenter should be held responsible for implementing profile editing and ensuring that consumer inspired corrections last long enough to make them worthwhile, e.g. 6 months for ordinary information and, for privileged information, 18 months, i.e. its maximum lifespan.

Competition makes it likely that an elementary profile information is given by its originator to more than one data aggregator, each serving many presenters. Getting one presenter to correct the profile it uses on a consumer is not practical enough for this consumer since it would affect only one data aggregator. The redress process must ensure the correction is quickly propagated to all other aggregators. Since the originator benefits from serving multiple aggregators, it must bear the responsibility to log and synchronize their copies upon request from a consumer or, as the case may be, from an arbitrator.

Once again it is very easy for consumers to spot and document either the lack or the failure of a redress process and ascertain responsibilities. If it concerns modifiable information within the profile accessed through a specific presenter, it is the responsibility of this presenter. If it concerns non modifiable information or the same information from the same originator but in a profile accessed through another presenter, it is the responsibility of the originator of this information.

- measure 4: protecting the consumer- nature of the threats

The previous measures are meant to give the consumer the possibility to see and rectify the personal profile which is used, directly or indirectly, by the presenters. Unfortunately profile errors are not the only threat consumers face with the advent of targeted advertising.

All online information is at risk of leaking over time through a mix of technical flaws and unsufficiently trained or rogue employees to third parties ready to break the law for their own benefit. With respect to a detailed consumer profile, ill intent includes discriminating against the consumer or intimidating the consumer. For instance employers are known to discriminate against prospective employees, landlords against prospective tenants, criminal gangs to extort protection money against exposed targets. Measure 4 proposes a test to determine what profile information generates a significant risk.

To downplay these risks would be reckless. By encouraging the collection of personal information and its aggregation into personal profiles, even under the cover of anonymity, presenters must acknowledge they create new risks and accept the responsibilities of their decisions.

- measure 4: protecting the consumer- reestablishing market balance

Consumer profiles have been accessible online for many years. What difference targeted advertising makes besides a quantitative increase in consumer risks? One only needs to track down who benefits. In principle at least, when a company feeds consumer information into its operational database, the operations of the company are for the satisfaction of the consumers concerned, who in return pay the company for its goods or services. When it uses consumer profiles to present targeted advertising, a presenter is not satisfying the consumer but the advertiser. It is the advertiser, not the consumer, who pays the presenter for the service rendered. In other words presenters benefit and consumers carry the risks.

According to the laws of economics, a market imbalance arises whenever the agent who receives the benefits from an act is distinct from the agent who bears the associated costs.

Presenters will of course spend money to protect the databases necessary to implement targeted advertising. Unfortunately this merely creates an additional market imbalance as these costs will be entirely supported by the presenters while the benefits accrue to the consumers.

Economics dictate that presenters maximize their profits, i.e. targeted advertising sales, and minimize their costs, i.e. consumer database protection. The more they do so, the worse off the consumers. The same is true for all the others organizations involved in targeted advertising, from originators to aggregators.

The solution to such a structural market failure is to remove the consumer profile database from the control of the organizations which will benefit from targeted advertising, i.e. presenters, originators, aggregators, their agents and intermediaries. This can only be done in one of two ways. Hand over the control to the consumers themselves or to FTC approved trusted third-parties, whose sole role will be to hold the consumer profile in escrow.

To give the consumer the material and exclusive control of his or her profile creates a balanced market by definition. As a result, risks and benefits of targeted advertising will be optimally apportioned between consumers, presenters and originators.

If an escrow receives the material and exclusive control of some consumer population, competition among escrows will also ensure balance. It will indeed dictate that cost minimization by an escrow be balanced by its goal to maximize revenues, which comes solely from protecting consumer information. From the perspective of the clients, whether presenters or aggregators, paying for the services of an escrow is equivalent to paying a premium to an insurer in exchange of bearing the associated risks.

- measure 4: protecting the consumer- implementation

Whether a single profile or a whole database, profile management run as an independent operation is the same:
- receive data from originators and record it
- receive ad requests from presenters or their ad suppliers, filter them against the profile(s) and return whether or not there is a match
- let consumers review their profile

Protecting a profile or a profile database against technical flaws and hackers, plus as the case may be deficient escrow employees, is a matter of ordinary due diligence. Beyond it however a special need exists to protect the profile from unlawful requests from unscrupulous advertisers, for example an employer targeting an advertisement to prospective candidates based on age or sex. The difficulty is again one of pattern recognition. An employer may not brazenly target men in their twenties but rather slyly eliminate consumers tracked to a Viagra online shop or to Cosmopolitan.

Given the growth potential of targeted advertising, it is not practical to rely on the good will of advertisers, nor on manual verification. In particular consumers who are the victims of discrimination cannot spot it. The only practical solution is to require the whole process of targeted advertising be formalized in a way which automatically guarantees the absence of discrimination and can be audited by an external auditor approved by the FTC.

To avoid technology dependence, measure 4 does not specify how to implement it. It is nevertheless quite feasible to satisfy this requirement. For example all targeted ads may be required to fall into predefined categories, auch as "cars", "cellular phone services", "jobs", and within each such category targeting may be restricted to predefined sets of lawful criteria. As a result it is easy to automatically deny an employer the use of age and sex-related criteria for targeting an "emergency room nurse position" ad.

In the previous example, a rogue employer may still try to pass such a job ad in the category "cars". In so doing he or she might be able to seek "20 to 30 year old females" but will be deprived of most of the criteria critical to an effective targeting of candidates for the position concerned, such as diploma and professional experience. In such a case the targeting request satisfies measure 4 in form only, but also allows the perversion to be formally documented to prove the intent to discriminate. This cleanly shifts the responsibility from presenters and puts it where it belongs, at the advertiser's door.

- do these measures fulfill all conditions?

Being concerned with the protection of consumers against deceit and abuse, including discrimination and intimidation, the four measures are well within the FTC remit.

ePrio

Second no specific technology has been specified by the measures.This is in fact true for both the solution and the problem. As it develops, targeted advertising will use any number of media such as Internet, phones, cable networks, and any number of consumer profiling techniques, such as search engines, social networks, browsing history aggregators. As long as the result is to present a targeted ad to the consumer online, the solution proposed should be applicable.

Third great pains have been taken to insure costs are born by those who benefit. In particular the extra costs to the FTC of implementing these measures would be negligible. While it is not possible to assert that costs have been made commensurate to benefits without carrying a quantitative assessment of an actual implementation, I firmly believe that it is the case based on my experience in the field.

Fourth are these measures practical? Notice that, for each measure, responsibility is clearly attributed, with a verification process, backed by actors who do not have an inherent conflict of interest.

The only question left is whether this solution is technically possible. I offer three arguments in support of a positive answer.

- the fact that so many companies are pressing ahead with targeted advertising proves that the managing of large customer profile databases is indeed cost effective. The measures proposed, especially measure 1, do not add much of an overhead to this base

- the adoption of HIPAA laws and regulations, which governs health-related data in the US, and the use of so-called trusted third parties, called for by European laws on consumer protection, prove that the measures proposed, are grounded in current, practical trends for a greater protection of consumer information as illustrated by measures 2 to 4. Check for example HIPAA requirements for external audits and the role of escrows as trusted third-parties

- my own experience points to a very inexpensive implementation based on incorporating a downloadable module onto the electronic device used by the consumer. This module gives total control of his or her profile to the consumer, while enabling the originators to deposit data into the profile, advertisers to send their targeting criteria to be matched, or not, against the profile and presentors to request the display of successful matches. Since, in the absence of explicit permissions, no one besides the consumer has access to any of the profile information and yet matches can still be determined as needed, this approach implements targeted advertising with little overhead from either the consumer or the other actors. In particular it allows measure 4 to do without an escrow and turns measure 1 into a simple local task.

One last point should be mentioned. Whenever targeted advertisement is used without requiring the consumer to sign in onto some site, it is obvious that the profile to be presented to the consumer must be based on other factors, such as the IP address of the consumer computer, which may or not provide a valid identification. As long as the profile to which the consumer has access is the same as the one used for targeting, this lack of precision does not invalidate the measures proposed. In fact letting the real consumer access the underlying profile can only lead to a greater level of precision.

ePrio Inc. - 14 Barbara D Lane - Tewksbury, MA 01876 - Phone/Fax: 1-978-658-7801 - philippe.coueignoux@eprivacy.com